AMENDMENTS TO THE SPECIFICATION

Please replace the following paragraphs.

On page 2, in the paragraph beginning on line 15 and ending on line 22:

- The writing of the signature is made in two stages. First of all, the message is reduced, known as ~~"hatched",~~ "hashed," by means of a sole direction reduction algorithm, such as those known under the names of SHA1 or MD5. Then the reduced message is encrypted by public key algorithm, for example RSA[[,]] or ECC ~~for example~~, with the aid of the private key of the signer. The result of this encrypting constitutes the signature.

On page 4, in the paragraph beginning on line 17 and ending on line 20:

As a protected cryptographic processing device, it is possible to use a microprocessor card, also called a microchip card. Regarding ~~As regards~~ the signature of a message, the microchip card offers the following services:

On page 5, in the paragraph beginning on line 6 and ending on line 11:

With this system, the signer ~~singer~~ is sure that nobody other than he can use his private key for signing. This solution is currently used and is sufficient for calculating the signature whose range has no legal value but for protecting a closed set of computers, such as the internal networks of large concerns.

On page 5, in the paragraph beginning on line 27 and ending on page 6, line 5:

Also, the technical problem to be resolved by the object of the present invention is to provide a method for checking the signature of a message, the message, signature and a certificate having been sent by a signer possessing a public key to a recipient having a message storage device for putting right the drawbacks of known cryptographic processing systems so as to attain a suitable level of protection to give the message sent an indisputable legal value and enable a recipient to check the identity of the signer and ensure that the latter is unable to revoke the message he has sent.[[.]]

On page 8, in the paragraph beginning on line 10 and ending on line 22:

The central unit 11 is connected by a linking cable 15 to a protected cryptographic processing device 21, in this case constituted by a microprocessor card placed in a box 22. As shown on figure 2, said box 22 includes an interface circuit 221 called a data/command circuit. The message needing to be signed or the message whose signature needs to be checked, as well as the data required for the checking or signature operations, arrive from the storage device 11 at the microchip card 21 via this circuit by observing, for example, the standard ISO 7816. The data/command circuit 221 has an ~~inlet~~ input by activating a button 222 for receiving a signal for triggering the signature operation and the data on a keyboard 224 of the box, such as a confidential code.

On page 9, in the paragraph beginning on line 5 and ending on line 17:

The ~~inlets/outlets~~ inputs/outputs of the commands/data 221 and display 223 circuits are electrically independent when no microprocessor card is present in the box 22. When a card 21 is inserted into the box 22, the electric earth is then shared between the two circuits 221 and 223. The data derived from the card 21 towards the display circuit 223 come out via a specific ~~outlet~~ output O_2 physically distinct from the ~~outlet~~ output O_1 used for the transfer of commands/data. Similarly, the commands/data and display ~~inlets~~ inputs I_1 and I_2 of the card 21 are physically separate. In fact, the only logic link between the data circulating in the data/commands 221 and display 223 circuits is the software of the card, considered as "extremely certain".

On page 10, in the paragraph beginning on line 7 and ending on line 12:

4. During arrival of the message coming from the storage device 11, the software 211 of the card 21 calculates from this on-line reduction and recopies it onto the display ~~outlet~~ output 0_2, so that the display device 30 could display, that is print, the message during the reduction operation.

On page 10, in the paragraph beginning on line 17 and ending on line 21:

6. The signer has the time to authenticate the printed message, and then if he accepts its contents, write said command message in the form of a confidential code entered on the keyboard 224 of the box 22. The data/commands circuit 221 generates the command for encrypting the reduced message by displaying the command and the confidential code entered on the keyboard 224 by the signer. The computer cannot see the contents of this command. It is also possible to have available a physically separate ~~inlet~~ input on the microprocessor card 21 so as to re-enter the confidential code.